Amendments to the Claims

Please replace all existing claims in the application with the following claims:

1. (Currently Amended) A method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of:

generating a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document;

encrypting the original document with the session key to create an encrypted document;

generating a proxy key based on a public key corresponding to the selected recipient, wherein the proxy key may be published without compromising its security, and wherein the proxy key is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process; and

applying the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the transformation may occur in an untrusted environment without compromising its security, and wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

2. (Original) The method of claim 1, further comprising the step of transmitting the transformed document to the selected recipient.

3. (Previously Presented) The method of claim 1, further comprising the steps of:

recovering the session key from the transformed document; and

decrypting the transformed document with the session key to recover the original document.

4. (Original) The method of claim 3, wherein the recovering step is performed by applying a private key corresponding to the selected recipient.

5. (Previously Presented) The method of claim 1, wherein the encrypting step is performed with a combination of a symmetric private-key encryption scheme and an asymmetric public-key encryption scheme.

6. (Previously Presented) The method of claim 5, wherein the asymmetric public-key encryption scheme is based on the ElGamal cryptosystem.

7. (Previously Presented) The method of claim 5, wherein the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private-key encryption scheme using the session key, and a second portion representative of the session key encrypted using an owner's private key according to the asymmetric public-key encryption scheme.

8. (Previously Presented) The method of claim 1, wherein the original document is distributed to the selected recipient through at least one additional intermediate grantor by repeating the following steps for each additional intermediate grantor:

generating a new proxy key based on the intermediate grantor's public key; and

transforming the encrypted document with the new proxy key to create a transformed document customized for the intermediate grantor.

9. (Previously Presented) The method of claim 1, wherein the encrypted document has been encrypted with a Cramer-Shoup encryption scheme.

10. (Previously Presented) The method of claim 5, wherein the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private-key encryption scheme using the session key, and a second portion

representative of the session key encrypted using an owner's private key according to the asymmetric public-key encryption scheme.

11. (Previously Presented) The method of claim 1, wherein the encrypted document has been encrypted with a modified ElGamal encryption scheme.

12. (Previously Presented) The method of claim 1, wherein the steps of generating a session key, encrypting the original document, generating a proxy key, and transforming the encrypted document are performed by the grantor.

13. (Currently Amended) A system operable to encrypt an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising:

a session key generation system that generates a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document;

an encryption system that encrypts the original document with the session key to create an encrypted document;

a proxy key generation system that generates a proxy key based on a public key corresponding to the selected recipient, wherein the proxy key may be published without compromising its security, and wherein the proxy key is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process; and

a transformation system that applies the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the transformation may occur in an untrusted environment without compromising its security, and wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

14. (Previously Presented) The system of claim 13, further comprising a transmitting system that transmits the transformed document to the selected recipient.

15. (Previously Presented) The system of claim 13, further comprising:

a recovering system that recovers the session key from the transformed document; and

a decrypting system that decrypts the transformed document with the session key to recover the original document.

16. (Previously Presented) The system of claim 13, wherein the recovery of the session key is performed by applying a private key corresponding to the selected recipient.

17. (Previously Presented) The system of claim 13, wherein the encryption is performed with a combination of a symmetric private-key encryption scheme and an asymmetric public-key encryption scheme.

18. (Previously Presented) The system of claim 17, wherein the asymmetric public-key encryption scheme is based on the ElGamal cryptosystem.

19. (Previously Presented) The system of claim 17, wherein the encrypted document comprises a first portion representative of the original document encrypted via the symmetric private-key encryption scheme using the session key, and a second portion representative of the session key encrypted using an owner's private key according to the asymmetric public-key encryption scheme.

20. (Previously Presented) The system of claim 13, wherein the original document is distributed to the selected recipient through at least one additional intermediate grantor by using the proxy key generation system to generate a new proxy key based on the intermediate grantor's public key, and using the transformation system to transform the encrypted document with the new proxy key to create a transformed document customized for the

intermediate grantor.

21. (Previously Presented) The system of claim 13, wherein the encrypted document has been encrypted with a Cramer-Shoup encryption scheme.

22. (Previously Presented) The system of claim 13, wherein the encrypted document has been encrypted with a modified ElGamal encryption scheme.